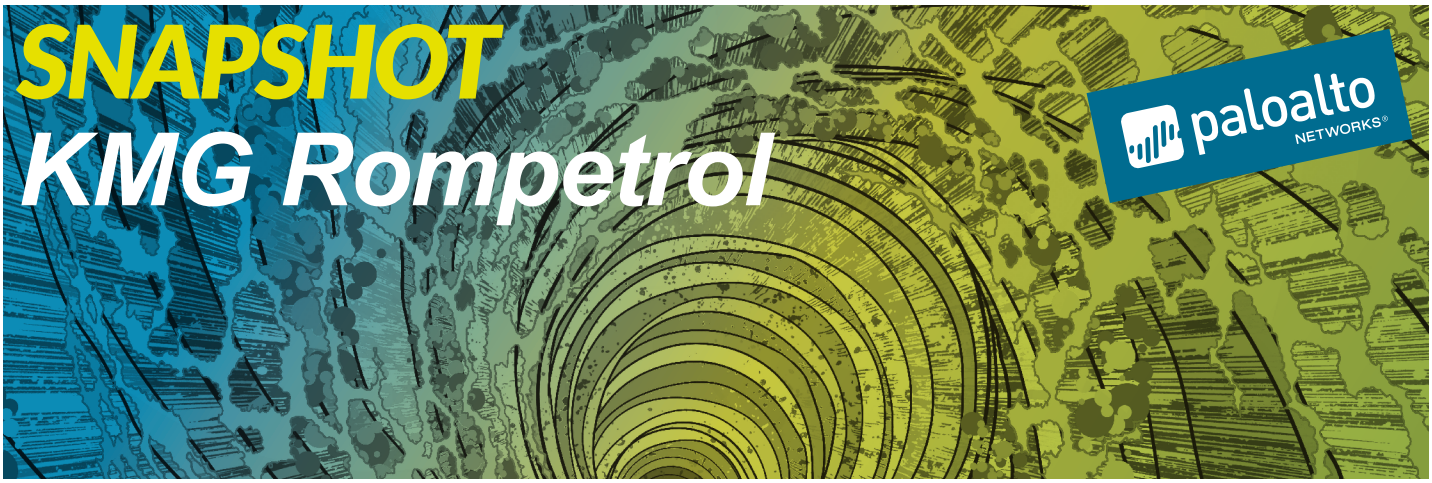

rompetrol

KMG Rompetrol Improves Endpoint Security and Reduces Malware Attacks

Industry
Oil and Gas

Challenge
Improve endpoint information security to combat malware and provide increased threat visibility.

Solution
Palo Alto Networks® Traps™ advanced endpoint protection creates a single dashboard for the rapid identification and elimination of threats that originate on endpoints.

Results

- More than 3,000 workstations and 650 servers secured with Traps.
- Approximately a 15 percent increase in detection rate – thereby reducing vulnerabilities and increasing endpoint security.
- Increased assets visibility achieved through use of a centralized dashboard.
- Improved availability and productivity through faster threat detection.

KMG Rompetrol conducts major operations in refining and petrochemicals, retail, trading, upstream, and industrial services in 11 main markets in Europe and Central Asia. In Romania, the group operates Petromidia Năvodari Refinery, with a processing capacity of more than 5 million tons per year; Vega Ploiesti Refinery, the oldest unit of its kind, in operation since 1905; a fuel distribution network of more than 716 distribution points under the Rompetrol brand; and 10 warehouses, 230 LPG supply stations, and 9,000 distribution points for gas tanks.

Diversifying its operations, the company has found itself relying more and more on tightly integrated business applications. A pioneer in adopting virtualization and using state-of-the-art technology to propel business, it recently created a dedicated cybersecurity division. The mandate of this division is to secure the operation of a reliable cyber protection platform while also focusing on prevention and organizational alignment practice.

In 2016, the company underwent a significant transformation in how it handled cybersecurity tasks at a group level, which saw IT security brought together under the umbrella of a new group function closer to the core business management. It also gave KMG the opportunity to re-evaluate its approach to information security.

“It was of paramount importance to shift the paradigm from IT security, which is limited to the technological side, and extend it to cover the CIA triad,” explains Victor Ciurus, group information security lead for KMG Rompetrol, referring to the three core goals of InfoSec: confidentiality, integrity and availability. “We have many different platforms, technologies and services within a heterogeneous landscape spread out across the country and abroad, which opens us up to a large number and variety of threats.”

“The level of information is much more detailed, making the interception of malware much simpler. It also allows us greater visibility over what files users are running and to block them if need be. Palo Alto Networks Traps also integrates seamlessly with McAfee and Defender, so we get a clear view of every endpoint.”

Victor Ciurus | group information security lead | KMG Rompetrol

One of the key objectives behind introducing a new layer of security was to provide centralized threat visibility to end-user devices, thus enabling the quick resolution of any possible incident.

“The management of endpoint protection was just these two solutions, but we couldn’t properly manage them in a centralized manner, which made it difficult to manage infections at source. At times, I was stunned to see malware getting by,” adds Ciurus. “There was no integration between the antivirus solutions we operated and our event management processes, which is why we went looking for a new solution to take us to the next level.”

Over the course of six months, Palo Alto Networks Traps Advanced Endpoint Protection has been deployed on over 650 servers and 3,000 workstations on a five-year contract with Premium Support for the duration. There are also plans to further extend the coverage of Traps advanced endpoint protection within Rompetrol’s infrastructure.

Centralized Visibility Improves Efficiency

Traps provides a single pane of glass through which to view the computing infrastructure in its entirety and extract information at a far more granular level. This allows companies to detect and remove threats more quickly, improving availability and user productivity.

“The level of information is much more detailed, making the interception of malware much simpler,” explains Ciurus. “It also allows us greater visibility over what files users are running and block them if need be. Palo Alto Networks Traps also integrates seamlessly with McAfee and Defender, so we get a clear view of every endpoint.”

“There should be a human resource load balance in checking incidents, and Palo Alto Networks Traps lets us flexibly split responsibilities and monitor them across a central dashboard,” says Ciurus.